



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,521	08/01/2003	Kim Cameron	MSI-1553US	4349
22971 7590 11/16/2007 MICROSOFT CORPORATION ONE MICROSOFT WAY REDMOND, WA 98052-6399			EXAMINER TIMBLIN, ROBERT M	
			ART UNIT 2167	PAPER NUMBER
			NOTIFICATION DATE 11/16/2007	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

roks@microsoft.com
ntovar@microsoft.com
a-rydore@microsoft.com

Office Action Summary

Application No.

10/632,521

Applicant(s)

CAMERON ET AL.

Examiner

Robert M. Timblin

Art Unit

2167

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-11, 15-73 and 80-85 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-11, 15-73 and 80-85 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is responsive to application 10/632521 filed on 8/1/03.

Response to Amendment

Claims 1, 53-65 and 80-85 have been amended and claims 74-79 have been cancelled. Accordingly, claims 1-11, 15-73 and 80-85 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 53 is now accepted under statute 35 USC 101 as being a machine claim including a processor.

Claim 61 and accordingly its depending claims remain rejected under 35 U.S.C. 101 because they are interpreted to be software per se (i.e. a program listing). Specifically, an interface as defined in Applicant's specification at page 5 line 4-7 defines an interface as an API, which is construed as software. As claim 61 is interpreted to be a machine claim, and is a computer related invention, it is construed to be software. Refer to MPEP 2106.01 where it states:

Computer programs claimed as computer listings per se, i.e., the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the

Art Unit: 2167

computer program and other claimed elements of a computer which permit the computer program's functionality to be realized.

Claim 83 is now accepted under statute 35 USC 101 in view of Applicant's amendments.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-11, 15-20, 22-26, 28-69, 71-73, and 80-85 are rejected under 35 U.S.C. 102(e) as being taught by Stone et al ('Stone' hereafter) (U.S. Patent Application 2003/0233439). In the following citations and figures, Stone discloses:

With respect to claim 1, A method, comprising:

selecting multiple data sources (36, 50) connected to an identity integration system (figures 1, 4), wherein:

the identity integration system (figures 1, 4) includes a management agent (34, 38, 52) for each of the multiple data sources (36, 50) configured specifically for its respective data source (36, 50) to manage data communication (0062) between the identity integration system (figures 1, 4) and each respective data source (36, 50);

for at least some of the multiple data sources (36, 50) a management agent for the data source (36, 50) is configured with credentials (0029) to perform password management (0056,0061); and

for at least one of the multiple data sources (36, 50) a management agent (34, 38, 52) for the data source calls for custom logic (administrative file 24, 0021 and figure 2, drawing reference 514) configured as code (figure 10), from a custom logic source (figure 17, 0074 and drawing references 12, 14) outside the identity integration system (figures 1, 4), to perform password management (0051, 0061) for the data source (36, 50);

receiving a new password (0071) input by a user (e.g. administrator, 0071); and
performing an administrative password operation (0049; i.e. updating/changing user attribute data and 0071; i.e. establishing and updating a password) on a password (0071; e.g. a global password) associated with each of the selected multiple data sources (36, 50) to collectively update each said password (0071; e.g. a global password) to the new password (0071, i.e. updating a password and figure 3), wherein the password operation (0071; i.e. establishing and updating a password) is performed using the identity integration system (figures 1, 4).

With respect to claim 2, the method as recited in claim 1, further comprising:

determining an identity of a user (0026), wherein the multiple data sources (36, 50) are associated with the identity (figure 3, drawing references 522-524); and

querying (0093) the identity integration system (figures 1, 4) to find the multiple data sources (36, 50) associated with the identity (0042, 0071, e.g. administrative profile).

With respect to claim 3, the method as recited in claim 1, wherein the password operation comprises updating one or more passwords associated with the multiple data sources using joined objects across the multiple data sources, wherein the joined objects are stored in the identity integration system (0059).

With respect to claim 4, the method as recited in claim 3, wherein some of the multiple passwords are updated to new passwords that differ from each other (0029).

With respect to claim 5, the method as recited in claim 3, wherein each of the multiple passwords is updated to the same password (last 3 lines of 0029).

With respect to claim 6, the method as recited in claim 1, wherein the password operation comprises one of changing, setting and resetting the password (0071).

With respect to claim 7, the method as recited in claim 1, wherein each of the multiple data sources differ from others of the multiple data sources with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage (0045-0046).

With respect to claim 8, the method as recited in claim 1, wherein each of the multiple data sources differs in a connection to the identity integration system with respect to at least one of a protocol, a platform, a format, and a data transmission medium for data storage (0031).

With respect to claim 9, the method as recited in claim 1, wherein each of the multiple data sources uses a different password management function (0029, 0118).

With respect to claim 10, the method as recited in claim 9, wherein the identity integration system performs password management for each of the multiple data sources (0053).

With respect to claim 11, the method as recited in claim 1, wherein for at least some of the multiple data sources the identity integration system stores integrated 20 identity information to perform password management (figure 3, e.g. a global password).

With respect to claim 15, the method as recited in claim 1, further comprising using the identity integration system to produce a list of user accounts associated with the multiple data sources, wherein the user accounts on the list are eligible for password management (0078; i.e. listing a directory).

With respect to claim 16, the method as recited in claim 1, further comprising allowing access to the identity integration system through a web application for password management (0077; i.e. use of web pages).

With respect to claim 17, the method as recited in claim 16, wherein the selecting multiple data sources and the performing a password operation are performed on a website generated by the web application (0040; web browser).

With respect to claim 18, the method as recited in claim 17, wherein the web application accepts a password credential from a user to perform the password operation (0026).

With respect to claim 19, the method as recited in claim 17, wherein the web application verifies an identity of a user by asking the user questions (figure 20, drawing reference 5104), wherein if answers provided by the user are correct (drawing reference 5106) then the web application performs the password operation using the identity of a privileged user account (figure 20).

With respect to claim 20, the method as recited in claim 17, further comprising using the identity integration system to produce a list of user accounts displayable on

Art Unit: 2167

the website, wherein the user accounts are associated with the multiple data sources (0078).

With respect to claim 22, the method as recited in claim 17, further comprising communicatively coupling the identity integration system with the web application using an interface (figure 17, drawing references 22, 44, 90).

With respect to claim 23, the method as recited in claim 22, wherein the interface is publicly available (figure 17, drawing reference 44, 46).

With respect to claim 24, the method as recited in claim 22, wherein the interface allows a web application designer to customize the web application (0021).

With respect to claim 25, the method as recited in claim 22, wherein the interface 20 includes password management functions (0056).

With respect to claim 26, the method as recited in claim 22, wherein the interface is capable of being changed for an improved version of the interface that adds more password management functions while using the same web application and the same identity integration system (0084; i.e. establishing and modifying a user template).

With respect to claim 28, the method as recited in claim 27, wherein the interface is secured using a security group (0005).

With respect to claim 29, the method as recited in claim 28, wherein the interface is secured using a security group (0005) that allows both searching for a connector object (drawing reference 28, 0025) associated with a data source and setting a password for an object in the data source, wherein a connector object represents at least part of the data source in the identity integration system (0059).

With respect to claim 30, the method as recited in claim 1, wherein an identity of a user associated with the multiple data sources provides a security credential for 20 performing a password operation (0058).

With respect to claim 31, the method as recited in claim 17, wherein the web application produces a list of accounts associated with a user (0078, 0106).

With respect to claim 32, the method as recited in claim 31, wherein the web 5 application lists only accounts eligible for password management (0078).

With respect to claim 33, the method as recited in claim 17, wherein the web application adopts a web application behavior based on a configuration setting (0042).

With respect to claim 34, the method as recited in claim 33, wherein the configuration setting is stored in a configuration file (0042; e.g. user profile).

With respect to claim 35, the method as recited in claim 17, wherein the web application checks if one of the data sources is communicating before updating a 15 password associated with the data source (0060; i.e. identifying availability).

With respect to claim 36, the method as recited in claim 35, wherein the updating comprises one of changing and setting the password (0071).

With respect to claim 37, the method as recited in claim 17, wherein the web application checks if a connection to one of the data sources is secure before updating a password associated with the data source (0022, 0048).

With respect to claim 38, the method as recited in claim 37, wherein the updating comprises one of changing and setting the password (0071).

With respect to claim 39, the method as recited in claim 1, further comprising displaying a status for the password operation (0106, 0124).

With respect to claim 40, the method as recited in claim 39, further comprising displaying the status on a webpage (0077).

With respect to claim 41, the method as recited in claim 1, further comprising auditing the password operation (0028; i.e. success/error logs).

With respect to claim 42, the method as recited in claim 41, further comprising 15 maintaining a password management history for the password operation (0028; i.e. archiving the logs).

With respect to claim 43, the method as recited in claim 42, further comprising keeping the password management history in a connector space object, wherein the connector space object is included in the identity integration system (0025).

With respect to claim 44, the method as recited in claim 42, wherein the password management history includes a tracking identifier to an audit record of the password operation (0028).

With respect to claim 45, the method as recited in claim 41, further comprising maintaining a repository of audit records for password operations performed using the identity integration system (0082, drawing reference 42).

With respect to claim 46, the method as recited in claim 45, wherein an audit record for a password operation includes at least one of an identifier of a user

Art Unit: 2167

associated with the password operation, a tracking identifier to a web application initiating the password operation, a tracking identifier to a connector object associated with the password operation, a tracking identifier to a management agent associated with the password operation, a password operation identifier, a password operation status, a date, and a time (0028, 0082).

With respect to claim 47, the method as recited in claim 1, further comprising associating custom logic (24) with a password operation (figure 10), wherein the custom logic is executed after the password operation is performed (0052, 0074).

With respect to claim 48, the method as recited in claim 47, wherein the custom logic sends an email (0085).

With respect to claim 49, the method as recited in claim 47, wherein the custom logic logs password management activity (0028).

With respect to claim 50, the method as recited in claim 47, wherein the custom logic performs a password operation on a subsequent data source not connected to the identity integration system (figure 5).

With respect to claim 51, the method as recited in claim 1, wherein the password operation further comprises updating passwords in both secure and non-secure data sources (0048) within the multiple data sources (50, 36).

With respect to claim 52, the method as recited in claim 1, wherein the password operation further comprises updating passwords over both secure and non-secure 15 connections to the multiple data sources (0048).

With respect to claim 53, An apparatus comprising:

a processor (0004); and

a web application (0022, web browser) for password management executable on the processor having one or more modules including:

a user identifier (0019; account identifier) to find user identity information (0058) in an identity integration system (figures 1,4), wherein:

the identity integration system (figures 1,4) includes a management agent (34, 38, 52) for each of multiple data sources (36, 50) to manage data communication (0062) between the identity integration system (figures 1, 4) and each respective data source (36, 50); and

for at least one of the multiple data sources (36, 50) a management agent (34, 38, 52) for the data source (36, 50) calls for custom logic (administrative file 24, 0021) configured as code (figure 10), from a custom logic source (figure 17, 0074 and drawing

Art Unit: 2167

references 12, 14) outside the identity integration system (figures 1,4), to perform password management for the data source (36, 50);

identity information query logic (0078) to search information in the identity integration system (figures 1,4) for accounts (figure 3, 0118) associated with the user;

an account lister to display the accounts associated with the user (0017);

an account selector (0056; i.e. selecting resources) to designate at least some of the displayed accounts for password management (0121-0123; i.e. selecting desired resources);

a password inputter to determine a new password input (0071) by a user to associate with each designated accounts (0121-0123; i.e. selected desired resources); and

a password manager (figure 1, drawing reference 32) to collectively manage passwords for the designated accounts (0071; e.g. a global password) by requesting an update of a password associated with each designated account to the new password (0071, i.e. updating a password and figure 3), responsive to the user input (0071).

With respect to claim 54, the apparatus web application as recited in claim 53, wherein the identity integration system connects with diverse data sources, each data source having a different function for using password security (0029, 0118).

With respect to claim 55, the apparatus web application as recited in claim 53, further comprising an account status display to show selected accounts and a connection status of each account (0091).

With respect to claim 56, the apparatus web application as recited in claim 53, further comprising a password management status display to display a password management operation status for each account (0106, 0124).

With respect to claim 57, the apparatus web application as recited in claim 53, further comprising a status checker to verify connectivity and security of a connection between an account and the identity integration system (0022, 0048).

With respect to claim 58, the apparatus web application as recited in claim 53, further comprising a configuration reader to obtain behavior settings for the web application (0042).

With respect to claim 59, the apparatus web application as recited in claim 53, further comprising a custom logic executor to perform custom logic associated with a password management operation (0024, receiver 28).

Art Unit: 2167

With respect to claim 60, the apparatus web application as recited in claim 53, wherein the account lister lists only accounts eligible for password management (0078; i.e. listing a directory).

With respect to claim 61, An apparatus comprising:

an interface (drawing reference 22) for coupling an identity integration system (figure 1, 4) with a password management web application (drawing reference 26), comprising:

logic for communicating (0062) with the identity integration system (figures 1, 4), wherein:

the identity integration system (figures 1, 4) is capable of collectively updating a password (0071, e.g. global password) on multiple data sources (36, 50) that use various functions of password updating (0071; i.e. establishing and updating a password) responsive to input of a single new password by a user (i.e. administrator);

the identity integration system (figures 1, 4) includes a management agent (34, 38, 52) for each of the multiple data sources (36, 50) to manage data communication (0062) between the identity integration system and each respective data source (36, 50);

for at least some of the multiple data sources (36, 50) a management agent (34, 38, 52) for the data source (36, 50) is configured with credentials to perform password management (0056-0061); and

Art Unit: 2167

for at least one of the multiple data sources (36, 50) a management agent for the data source (36, 50) calls for custom logic (administrative file 24, 0021) configured as code (figure 10), from a custom logic source (figure 17, 0074 and drawing references 12, 14) outside the identity integration system (figures 1,4), to perform password management (0056-0061) for the data source (36, 50);

logic for communicating with the password management (0056-0061) web application;

logic for searching for objects (0078) in the identity integration system (figures 1,4); and

logic for checking a connection status (0091) between the identity integration system (figures 1,4) and a data source (36, 50).

With respect to claim 62, the apparatus interface as recited in claim 61, further comprising logic for checking security of a connection between the identity integration system and a data source (0022, 0048).

With respect to claim 63, the apparatus interface as recited in claim 61, further comprising logic to change a password associated with the data source (0071).

With respect to claim 64, the apparatus interface as recited in claim 61, further comprising logic to set a password associated with the data source (0071, i.e. updating a password).

With respect to claim 65, password management system, comprising:

an identity integration system having (figures 1, 4) a metaverse space (40, 36, 50) for persisting integrated identity information (0042; e.g. user profiles) regarding accounts (figure 3, 0118) associated with a user, and a connector space (0025) for persisting information representing multiple data sources (36, 50) connectable to the identity integration system (figures 1, 4), the accounts each corresponding (figure 3) to one of the multiple data sources (36, 50) and having associated manageable passwords (e.g. global password);

for at least one of the multiple data sources (36, 50), a management agent (34, 38, 52) for the data source configured to call for custom code, (administrative file 24, 0021) configured as code (figure 10), from a custom logic source (figure 17, 0074 and drawing references 12, 14) outside the identity integration system (figures 1,4), to perform password management (0051, 0061) for the data source (36, 50);

a web application (26) for producing a list of the accounts (0078; i.e. listing a directory) from the identity integration system, for allowing selection of at least some of the accounts, for inputting by a user of a new password (0071) to cause the new password to be associated with each of the selected accounts (0071; i.e. establishing and updating a password), and for requesting the identity integration system (figures 1,4) to collectively update passwords (0071; e.g. a global password) on each of the selected accounts based on to the input new password (0071, i.e. updating a password and figure 3); and

Art Unit: 2167

an interface to communicatively couple the identity integration (figures 1, 4) system with the web application (0026).

With respect to claim 66, the password management system as recited in claim 65, wherein the password management web application verifies one of an identity and a credential of a user (0027).

With respect to claim 67, the password management system as recited in claim 65, wherein the web application generates a webpage (0077) that displays accounts and a status of a password management operation for each account displayed (0106, 0124).

With respect to claim 68, the password management system as recited in claim 65, wherein the web application operates in a security context (0005).

With respect to claim 69, the password management system as recited in claim 68, wherein the security context is an application pool identity (0005; i.e. user groups).

With respect to claim 71, the password management system as recited in claim 65, wherein the identity integration system stores a password management operation history for each account (0028; i.e. log archives).

With respect to claim 72, the password management system as recited in claim 65, wherein the identity integration system communicates with diverse accounts, each account having a different mechanism for administering a password associated with the account (0029, 0118).

With respect to claim 73, the password management system as recited in claim 72, wherein the identity integration system does not natively communicate with at least some of the diverse accounts (0045-0046).

With respect to claim 80, A computer-implemented method comprising:

Retrieving a list of user accounts (fig. 11) from an identity integration system (figures 1, 4) having persisted identity information (0042; e.g. user profiles) regarding the user accounts (0088) wherein, the identity integration system (figures 1,4) includes a management agent (34, 38, 52) for each of multiple data sources (36; 50) configured specifically for its respective data source (36, 50) to manage data communication (0062) between the identity integration system (figures 1,4) and each respective data source (36, 50);

outputting a user interface (figure 11) showing the list of user accounts (user list) on a display (12);

allowing each account in the list (e.g. user in the user list) to be selected using a user interface selection device (0083) operable to input selections via the user interface output on the display (12);

Art Unit: 2167

allowing input of a new password (0071) via the user interface selection device (0083, 0112); and

allowing input of a request (0112; a request to manage an attribute of a user) to update old passwords (0071; i.e. updating password) associated with each of the selected accounts (figure 11, user accounts/profiles) to the new password input via the user interface (figure 11).

With respect to claim 81, the method as recited in claim 80, further comprising allowing input of user credentials to verify an identity of the user (0027).

With respect to claim 82, One or more computer readable storage media containing instructions that are executable by a computer to perform actions, comprising:

selecting multiple data sources (36, 50) connected to an identity integration system (figures 1, 4);

receiving a new password (0071) input by a user (e.g. administrator) to cause the new password to be associated with each of the selected multiple data sources (0049; i.e. updating the affected resources); and

for at least one of the multiple data sources (36, 50), using the identity integration system to collectively update a password (0071; e.g. a global password) associated with each of the selected multiple data sources (36, 50) to the new password input by the user (0071).

With respect to claim 83, the one or more computer readable storage media as recited in claim 82, wherein at least some of the multiple data sources (36, 50) connected to the identity integration system communicate in a manner different than a native communication of the identity integration system (0045-0046).

With respect to claim 84, the one or more computer readable storage media as recited in claim 82, wherein the identity integration (figure 1,4) system accomplishes a password update (0071) on each of the data sources (36, 50) regardless of whether the data sources connected to the identity integration system communicate in a manner different than a native communication of the identity integration system (0049).

With respect to claim 85, the one or more computer readable storage media as recited in claim 84, wherein the identity integration system accomplishes a password update on at least one of, an ACTIVE DIRECTORY® data source, a SUN ONE server data source, a LOTUS NOTES server data source, a WINDOWS® NT TM server data source, a NOVELL® EDIRECTORY TM server data source, and a flat file data source (0032; e.g. Novell directory service NDS).

Claim Rejections - 35 USC § 103

Art Unit: 2167

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 21 and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stone as applied to claims 1-11, 15-20, 22-26, 28-69, 71-73, and 80-85 above in view of Bush et al. ('Bush' hereafter) (U.S. Patent Application 2002/0083012).

With respect to claim 21 and similar claim 70, Stone fails to teach a help desk to at least assist in the performing a password operation.

Bush, however, teaches a help desk to at least assist in the performing a password operation (0024, i.e. sending a password by telephone to the user) for assisting in new user registration.

In the same field of endeavor, (i.e. password management), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Bush's system would have given Stone's system a more user friendly and efficient method of helping a user to establish an account.

With respect to claim 70, Stone fails to teach the password management system as recited in claim 69, further comprising a help desk application, wherein the web

Art Unit: 2167

application denies a user access to the help desk application if a security group of the user is not approved by the web application.

Bush, however, teaches a help desk application, wherein the web application denies a user access to the help desk application if a security group of the user is not approved by the web application (0024, and 0039) for assisting in new user registration.

In the same field of endeavor, (i.e. password management), it would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references because Bush's system would have given Stone's system a more user friendly and efficient method of helping a user to establish an account.

Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stone as applied to claims 1-11, 15-20, 22-26, 28-69, 71-73, and 80-85 above in view of Davis et al. ('Davis' hereafter) (U.S. Patent 6,976,262).

With respect to claim 27, Stone fails to teach wherein the interface is a WINDOWS MANAGEMENT INSTRUMENTATION interface.

Davis, however, teaches wherein the interface is a WINDOWS MANAGEMENT INSTRUMENTATION interface as a WBEM system (col. 4 lines 62-62) to perform object management operations.

It would have been obvious to one of ordinary skill in the data processing art at the time of the present invention to combine the teachings of the cited references

Art Unit: 2167

because Davis would have given Stone a standard for managing systems, networks, users, and applications y using Internet technology (col. 1 lines 40-50, Davis).

Response to Arguments

Applicant's arguments with respect to claims 1-11, 15-73, and 80-85 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed; and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.


Contact Information


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert M. Timblin whose telephone number is 571-272-5627. The examiner can normally be reached on M-F 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jean R. Homere can be reached on 571-272-3780. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Robert M. Timblin


Patent Examiner: AU 2167


Primary Examiner
AA Unit 2167